

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-85624

(43)公開日 平成11年(1999)3月30日

(51)Int.Cl.*

G 0 6 F 12/14

識別記号

3 2 0

F I

G 0 6 F 12/14

3 2 0 F

審査請求 未請求 請求項の数6 OL (全12頁)

(21)出願番号

特願平9-245457

(22)出願日

平成9年(1997)9月10日

(71)出願人 000206211

大成建設株式会社

東京都新宿区西新宿一丁目25番1号

(72)発明者 野村 亨右

東京都新宿区西新宿一丁目25番1号 大成建設株式会社内

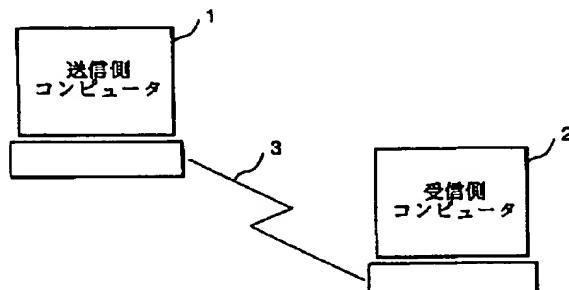
(74)代理人 弁理士 森 哲也 (外3名)

(54)【発明の名称】 データ保護装置

(57)【要約】

【課題】 クロックタイマ装置の時刻が変更されても、データが時間的に無制限に利用されるのを有効に防止し、もって作成者の利益を保護するのに好適なデータ保護装置を提供する。

【解決手段】 送信側コンピュータ1において、利用許可開始時刻および利用許可終了時刻を設定した利用許可時間データを保護対象データに関連付け、これを受信側コンピュータ2に送信し、受信側コンピュータ2において、関連付けられた利用許可時間データに基づいて、クロックタイマ装置6から出力される時刻が利用許可時間幅にないときには、保護対象データを消去する。



1

【特許請求の範囲】

【請求項1】 コンピュータに適用され、クロックタイマ装置から出力される時刻に基づいて、所定時刻を超過した保護対象データを消去するようになっているデータ保護装置において、

データの利用許可を開始させる利用許可開始時刻及びデータの利用許可を終了させる利用許可終了時刻を特定するための利用許可時間データを前記保護対象データに関する利用許可時間データ関連付手段と、関連付けられた前記利用許可時間データに基づいて、前記クロックタイマ装置から出力される時刻が前記利用許可開始時刻よりも前であるとき、又は前記利用許可終了時刻よりも後であるときには、前記保護対象データを消去する保護対象データ消去手段と、を備えることを特徴とするデータ保護装置。

【請求項2】 前記利用許可時間データ関連付手段は、複数の前記利用許可時間データを前記保護対象データに関する利用許可時間データのうち利用許可時間幅が最短となる前記利用許可時間データに基づいて、前記保護対象データの消去を判定するようになっていることを特徴とする請求項1記載のデータ保護装置。

【請求項3】 前記利用許可時間データ関連付手段を、送信側コンピュータに設け、前記保護対象データ消去手段を、ネットワークを介して前記送信側コンピュータに接続された受信側コンピュータに設けることを特徴とする請求項1又は2記載のデータ保護装置。

【請求項4】 データを送信する送信側コンピュータと、前記送信側コンピュータから送信されたデータを受信する受信側コンピュータと、が接続されたネットワークに適用され、所定時刻を超過した保護対象データを消去するようになっているデータ保護装置において、データの利用許可を開始させる利用許可開始時刻及びデータの利用許可を終了させる利用許可終了時刻を特定するための利用許可時間データを前記保護対象データに関する利用許可時間データ関連付手段を、前記送信側コンピュータに設け、

前記保護対象データを受信したときに前記保護対象データに少なくとも1つの前記利用許可時間データを関連付ける第2の利用許可時間データ関連付手段と、前記複数の利用許可時間データのうち利用許可時間幅が最短となる前記利用許可時間データに基づいて、前記クロックタイマ装置から出力される時刻が前記利用許可開始時刻よりも前であるとき、又は前記利用許可終了時刻よりも後であるときには、前記保護対象データを消去する保護対象データ消去手段と、を前記受信側コンピュータに設けることを特徴とするデータ保護装置。

【請求項5】 前記利用許可時間データ関連付手段は、前記保護対象データの作成者又は所有者の意思に応じて、少なくとも前記利用許可開始時刻及び前記利用許可

2

終了時刻のいずれか一方を可変に設定するようになっていることを特徴とする請求項1、2、3又は4記載のデータ保護装置。

【請求項6】 前記利用許可時間幅を短縮する方向で、前記利用許可時間データにより特定される前記利用許可開始時刻を、前記クロックタイマ装置から出力される時刻又はそれ以前の時刻に再設定するようになっていることを特徴とする請求項1、2、3、4又は5記載のデータ保護装置。

10 【発明の詳細な説明】

【0001】

【発明の属する技術の分野】 本発明は、利用許可時間を超過しているデータを消去するデータ保護装置に係り、特に、データが時間的に無制限に利用されるのを好適に防止するデータ保護装置に関する。

【0002】

【従来の技術】 従来、データの利用を時間的に制限するようにしたデータ保護装置としては、次のようなものがある。

20 【0003】 まず、送信側コンピュータでは、送信者（例えば、データの作成者）が送信しようとする保護対象データについて、その利用を許可する利用許可時間を指定すると、データの利用許可を終了させる終了時刻を設定した終了時刻データが保護対象データに付加され、これが受信側コンピュータに送信される。

【0004】 そして、受信側コンピュータでは、受信者（例えば、作成者から保護対象データの利用を許諾された許諾者）が、受信した保護対象データを利用しようとしてアプリケーションプログラムを起動させると、コンピュータ内蔵のクロックタイマ装置から出力される時刻が、終了時刻データに設定された終了時刻を超過しているか否かが判定され、超過していると判定されたときは、その保護対象データが消去される。

【0005】

【発明が解決しようとする課題】 しかしながら、従来のデータ保護装置にあっては、クロックタイマ装置から出力される時刻が、終了時刻データに設定された終了時刻を超過しているか否かを判定していただけであったため、受信者によってタイマ装置の時刻が現在の時刻よりも前に設定されてしまうと、保護対象データの利用時間が実質的に延長されることになる。すなわち、上記のようにデータの利用を時間的に制限しようとしても、終了時刻よりも遙か前の時刻にクロックタイマ装置の時刻が設定されてしまえば、結局のところ、保護対象データが無制限に利用されることになってしまう。

【0006】 この場合特に、暗号化されるようなデータは、一般に機密度が極めて高いものであるため、設定した利用許可時間を超過して利用されると、データの作成者は、著しい損害を被る危険性にさらされる。

50 【0007】 そこで、本発明は、このような従来の問題

を解決することを課題としており、クロックタイマ装置の時刻が変更されても、データが時間的に無制限に利用されるのを有効に防止し、もって作成者の利益を保護するのに好適なデータ保護装置を提供することを目的としている。

【0008】

【課題を解決するための手段】上記目的を達成するため、本発明に係る請求項1記載のデータ保護装置は、コンピュータに適用され、クロックタイマ装置から出力される時刻に基づいて、所定時刻を超過した保護対象データを消去するようになっているデータ保護装置において、データの利用許可を開始させる利用許可開始時刻およびデータの利用許可を終了させる利用許可終了時刻を特定するための利用許可時間データを前記保護対象データに関連付ける利用許可時間データ関連付手段と、関連付けられた前記利用許可時間データに基づいて、前記クロックタイマ装置から出力される時刻が前記利用許可開始時刻よりも前であるとき、または前記利用許可終了時刻よりも後であるときには、前記保護対象データを消去する保護対象データ消去手段と、を備える。

【0009】このような構成であれば、保護対象データの利用を時間的に制限しようとするには、利用許可時間データ関連付手段で、利用許可時間データが保護対象データに関連付けられる。ここで、利用許可時間データは、利用許可開始時刻および利用許可終了時刻が保護対象データ消去手段で特定可能なデータであって、これには、例えば、利用許可開始時刻および利用許可終了時刻を設定したデータや、利用許可開始時刻および利用許可時間幅を設定したデータなどが挙げられる。

【0010】そして、保護対象データ消去手段では、関連付けられている利用許可時間データに基づいて、クロックタイマ装置から出力される時刻が、利用許可時間データにより特定される利用許可開始時刻よりも前であったり、または利用許可終了時刻よりも後であったりしたときに、保護対象データが消去される。

【0011】つまり、保護対象データは、例えば、アプリケーションプログラムを起動させるのに応じて、クロックタイマ装置の時刻が利用許可時間幅にあるか否かが判定され、利用許可時間幅にないと判定されたときに消去されたり、また例えば、クロックタイマ装置の時刻が利用許可時間幅にあるか否かを判定する割り込み処理を常に実行させておき、利用許可時間幅にないと判定されたときに消去されたりする。

【0012】このとき、クロックタイマ装置の時刻が利用許可開始時刻よりも前であるという状態は、利用許可時間データが関連付けられたのちに、クロックタイマ装置の時刻が変更されたものと考えられるので、利用許可時間を不正に延長しようとするものであると判定し、消去の対象にするものである。

【0013】この請求項1記載の発明において、利用許

可時間データを保護対象データに関連付けるとは、利用許可時間データを保護対象データの先頭や末尾に付加するとか、補助記憶装置における利用許可時間データが格納されている位置をリンク先として保護対象データの先頭や末尾に付加するとか、保護対象データと利用許可時間データとを対応テーブルで対応付けるとか、が挙げられる。

【0014】また、本発明に係る請求項2記載のデータ保護装置は、請求項1記載のデータ保護装置において、前記利用許可時間データ関連付手段は、複数の前記利用許可時間データを前記保護対象データに関連付けるようになっており、前記保護対象データ消去手段は、前記複数の利用許可時間データのうち利用許可時間幅が最短となる前記利用許可時間データに基づいて、前記保護対象データの消去を判定するようになっている。

【0015】このような構成であれば、保護対象データの利用を時間的に制限しようとするには、利用許可時間データ関連付手段で、複数の利用許可時間データが保護対象データに関連付けられる。

【0016】そして、保護対象データ消去手段では、関連付けられている複数の利用許可時間データのうち利用許可時間幅が最短となる、すなわち利用許可開始時刻と利用許可終了時刻との間隔が最短となる利用許可時間データが選択され、これに基づいて、保護対象データが消去される。

【0017】利用許可時間データが関連付けられている保護対象データは、あらかじめ設定した利用許可時間が超過した後は消去される。ところが、利用許可時間データを改ざんすることにより、利用許可時間を延長させることも可能である。この場合特に、利用許可時間データが一つしか関連付けられていないときには、利用許可時間データが改ざんされる可能性が極めて高い。

【0018】そこで、この請求項2記載の発明では、利用許可時間を不正に延長するのを防止するために、ダミーとなる複数の利用許可時間データを保護対象データに関連付けるようとする。そして、保護対象データを消去するか否かについて判定するときには、複数の利用許可時間データうち利用許可時間幅が最短となるものを選択し、これに基づいて行うようにすれば、例え複数の利用許可時間データのうちいずれかの利用許可時間データが利用許可時間を延長するよう改ざんされたとしても、すべての利用許可時間データが改ざんされない限り、あらかじめ設定した利用許可時間を超過して保護対象データが利用されることはない。

【0019】また、この場合において、利用許可時間データが改ざんされたことが検出されたときには、例えば、すべての利用許可時間データを利用許可時間幅が最短となる利用許可時間データに書き換えるようにしたり、保護対象データを消去したりするのが好ましい。

【0020】さらに、本発明に係る請求項3記載のデー

タ保護装置は、請求項1または2記載のデータ保護装置において、前記利用許可時間データ関連付手段を、送信側コンピュータに設け、前記保護対象データ消去手段を、ネットワークを介して前記送信側コンピュータに接続された受信側コンピュータに設ける。

【0021】このような構成であれば、送信側コンピュータにおいて、受信側コンピュータに保護対象データを送信しようとすると、利用許可時間データ関連付手段で、利用許可時間データが保護対象データに関連付けられ、受信側コンピュータに送信される。

【0022】そして、受信側コンピュータにおいて、このように利用許可時間データが関連付けられた保護対象データを受信すると、保護対象データ消去手段では、利用許可時間データに基づいて、クロックタイマ装置から出力される時刻が、利用許可時間データにより特定される利用許可開始時刻よりも前であったり、または利用許可終了時刻よりも後であったりしたときに、保護対象データが消去される。

【0023】さらに、本発明に係る請求項4記載のデータ保護装置は、データを送信する送信側コンピュータと、前記送信側コンピュータから送信されたデータを受信する受信側コンピュータと、が接続されたネットワークに適用され、所定時刻を超過した保護対象データを消去するようになっているデータ保護装置において、データの利用許可を開始させる利用許可開始時刻およびデータの利用許可を終了させる利用許可終了時刻を特定するための利用許可時間データを前記保護対象データに関連付ける利用許可時間データ関連付手段を、前記送信側コンピュータに設け、前記保護対象データを受信したときに前記保護対象データに少なくとも1つの前記利用許可時間データを関連付ける第2の利用許可時間データ関連付手段と、前記複数の利用許可時間データのうち利用許可時間幅が最短となる前記利用許可時間データに基づいて、前記クロックタイマ装置から出力される時刻が前記利用許可開始時刻よりも前であるとき、または前記利用許可終了時刻よりも後であるときには、前記保護対象データを消去する保護対象データ消去手段と、を前記受信側コンピュータに設ける。

【0024】このような構成であれば、送信側コンピュータにおいて、受信側コンピュータに保護対象データを送信しようとすると、利用許可時間データ関連付手段で、利用許可時間データが保護対象データに関連付けられ、受信側コンピュータに送信される。

【0025】そして、受信側コンピュータにおいて、このように利用許可時間データが関連付けられた保護対象データを受信すると、第2の利用許可時間データ関連付手段で、受信した保護対象データに少なくとも1つの利用許可時間データが関連付けられる。

【0026】次いで、保護対象データ消去手段では、関連付けられている複数の利用許可時間データのうち利用

許可時間幅が最短となる利用許可時間データが選択され、これに基づいて、クロックタイマ装置から出力される時刻が、利用許可時間データにより特定される利用許可開始時刻よりも前であったり、または利用許可終了時刻よりも後であったりしたときに、保護対象データが消去される。

【0027】さらに、本発明に係る請求項5記載のデータ保護装置は、請求項1、2、3または4記載のデータ保護装置において、前記利用許可時間データ関連付手段は、前記保護対象データの作成者または所有者の意思に応じて、少なくとも前記利用許可開始時刻および前記利用許可終了時刻のいずれか一方を可変に設定するようになっている。

【0028】このような構成であれば、利用許可時間データ関連付手段で、保護対象データの作成者または所有者が指定した利用許可開始時刻または利用許可終了時刻に基づいて、利用許可時間データが生成され、保護対象データに関連付けられる。

【0029】さらに、本発明に係る請求項6記載のデータ保護装置は、請求項1、2、3、4または5記載のデータ保護装置において、前記利用許可時間幅を短縮する方向で、前記利用許可時間データにより特定される前記利用許可開始時刻を、前記クロックタイマ装置から出力される時刻またはそれ以前の時刻に再設定するようになっている。

【0030】このような構成であれば、保護対象データに利用許可時間データが関連付けられたのちには、利用許可時間データにより特定される利用許可開始時刻が、利用許可時間幅を短縮する方向で、クロックタイマ装置から出力される時刻に再設定される。この場合に、利用許可開始時刻は、利用許可時間幅を短縮する方向であるならば、クロックタイマ装置から出力される時刻よりも前に再設定されてもよい。

【0031】利用許可時間データが関連付けられている保護対象データは、クロックタイマ装置の時刻が変更された場合、変更したのちの時刻が利用許可開始時刻よりも前であるときには、消去される。しかし、クロックタイマ装置の時刻が、利用許可終了時刻よりも前でかつ利用許可開始時刻よりも後である範囲内で変更されたときには、消去されない。このため、現在の時刻（クロックタイマ装置から出力される現在の時刻）よりも前でかつ利用許可開始時刻よりも後に変更されたときには、実質的に利用許可時間が延長されてしまうことになる。

【0032】そこで、請求項6記載の発明では、クロックタイマ装置から出力される時刻を参照し、その時刻が利用許可開始時刻と利用許可終了時刻との間にあるときには、利用許可開始時刻を現在の時刻よりも前、好ましくは現在の時刻に再設定するようにする。そうすると、あらかじめ設定された利用許可時間からすでに利用した利用経過時間を減算したものを新たな利用許可時間とし

て再設定することになり、この新たな利用許可時間に基づいて、保護対象データを消去するようすれば、クロックタイマ装置の時刻が変更されることにより、利用許可時間が不正に延長されるのを確実に防止することが可能となる。

【0033】

【発明の実施の形態】以下、本発明の第1の実施の形態を図面を参照しながら説明する。図1は、本発明に係るデータ保護装置による第1の実施の形態を示すブロック図である。

【0034】この第1の実施の形態は、本発明に係るデータ保護装置を、図1に示すように、送信側コンピュータ1から送信された保護対象データが、受信側コンピュータ2で時間的に無制限に利用されるのを防止するのに適用したものである。

【0035】図中、保護対象データを送信する送信側コンピュータ1と、保護対象データを受信する受信側コンピュータ2とは、データを伝送するためのデータ伝送路3で接続されている。

【0036】送信側コンピュータ1および受信側コンピュータ2は、図2に示すように、制御プログラムに基づいて演算およびシステム全体を制御する演算処理装置4と、電気的にデータの読み出しおよび書き込みが可能な主記憶装置5と、設定した時刻を基準として経過時間を計数するクロックタイマ装置6と、外部に接続される外部装置と主記憶装置5とのデータの入出力をを行う入出力制御装置7と、で構成されており、演算処理装置4と、主記憶装置5と、クロックタイマ装置6と、入出力制御装置7とは、データを伝送するための信号線であるバスで相互に接続されている。そして、入出力制御装置7には、外部装置として、磁気的にデータの読み出しおよび書き込みが可能な補助記憶装置8と、データの入力が可能なヒューマンインターフェースとしてのキーボード9と、データ伝送路3と、がそれぞれ接続されている。

【0037】主記憶装置5は、所定領域にあらかじめ演算処理装置4の制御プログラム等を格納しているROMと、ROMまたは補助記憶装置8から読み込んだデータや演算処理装置4の演算過程で必要な演算結果を格納するRAMと、で構成されている。

【0038】送信側コンピュータ1の演算処理装置4は、マイクロプロセッサユニットMPU等からなり、補助記憶装置8に格納されている保護対象データを送信しようとするときには、主記憶装置5のROMの所定領域に格納されている所定のプログラムを起動させ、図3のフローチャートに示す処理を実行するように構成されている。

【0039】ここで、送信側コンピュータ1の演算処理装置4において、保護対象データを送信しようとするときに実行される処理は、次のように構成されている。まず、図中、ステップS1では、送信しようとする保護対

象データの指定をキーボード9から入力し、ステップS2に移行して、指定された保護対象データの利用許可を開始させる利用許可開始時刻をキーボード9から入力し、ステップS3に移行して、指定された保護対象データの利用許可を終了させる利用許可終了時刻をキーボード9から入力し、ステップS4に移行するようになっている。

【0040】ステップS4では、入力した利用許可開始時刻および利用許可終了時刻を設定した利用許可時間データを生成し、ステップS5に移行して、生成した利用許可時間データを保護対象データの先頭に付加し、ステップS6に移行するようになっている。

【0041】ステップS6では、保護対象データを暗号化するための暗号キーをキーボード9から入力し、ステップS7に移行して、入力した暗号キーで保護対象データを暗号化し、ステップS8に移行して、暗号化した保護対象データを受信側コンピュータ2に送信し、一連の処理を終了するようになっている。

【0042】受信側コンピュータ2の演算処理装置4は、マイクロプロセッサユニットMPU等からなり、暗号化された保護対象データを入出力制御装置7で受信したときには、主記憶装置5のROMの所定領域に格納されている所定のプログラムを起動させ、図4(a)のフローチャートに示す処理を実行し、保護対象データを利用するアプリケーションプログラムを起動させるのに応じて、図4(b)のフローチャートに示す処理を実行するように構成されている。

【0043】ここで、受信側コンピュータ2の演算処理装置4において、暗号化された保護対象データを入出力制御装置7で受信したときに実行される処理は、次のように構成されている。

【0044】まず、図中、ステップS11では、受信した保護対象データを復号化するための復号キーをキーボード9から入力し、ステップS12に移行して、入力した復号キーで保護対象データを復号化し、ステップS13に移行して、復号化した保護対象データの先頭に利用許可時間データが付加されているか否かを判定し、付加されていると判定されたときには、ステップS14に移行するようになっている。

【0045】ステップS14では、付加されている利用許可時間データと同一の利用許可時間データを複数生成し、ステップS15に移行して、生成した利用許可時間データをそれぞれ個別のファイルとして補助記憶装置8に格納し、ステップS16に移行して、復号化した保護対象データを補助記憶装置8に格納し、一連の処理を終了するようになっている。

【0046】一方、ステップS13で、復号化した保護対象データの先頭に利用許可時間データが付加されていないと判定されたときには、ステップS16に移行するようになっている。

【0047】また、受信側コンピュータ2の演算処理装置4において、保護対象データを利用するアプリケーションプログラムを起動させるのに応じて実行される処理は、次のように構成されている。

【0048】まず、図中、ステップS21では、利用しようとする保護対象データを主記憶装置4のRAMに読み込み、ステップS22に移行して、保護対象データの先頭に利用許可時間データが付加されているか否かを判定し、付加されていると判定されたときには、ステップS23に移行して、すべての利用許可時間データを主記憶装置4のRAMに読み込み、ステップS24に移行して、複数の利用許可時間データのうち利用許可時間幅が最短に設定されている利用許可時間データを選択し、ステップS25に移行するようになっている。

【0049】ステップS25では、クロックタイマ装置6から出力される時刻を取得し、ステップS26に移行して、取得した時刻が選択した利用許可時間データに設定されている利用許可開始時刻よりも前であるか否かが判定され、前でないと判定されたときには、ステップS27に移行して、取得した時刻が選択した利用許可時間データに設定されている利用許可終了時刻よりも後であるか否かが判定され、後であると判定されたときには、ステップS28に移行するようになっている。

【0050】ステップS28では、保護対象データを消去し、ステップS29に移行して、アプリケーションプログラムを実行し、一連の処理を終了するようになっている。

【0051】一方、ステップS27で、取得した時刻が選択した利用許可時間データに設定されている利用許可終了時刻よりも後でないと判定されたときには、ステップS29に移行するようになっている。

【0052】また一方、ステップS26で、取得した時刻が選択した利用許可時間データに設定されている利用許可終了時刻よりも前であると判定されたときには、ステップS28に移行するようになっている。

【0053】また一方、ステップS22で、保護対象データの先頭に利用許可時間データが付加されていないと判定されたときには、ステップS29に移行するようになっている。

【0054】次に、上記第1の実施の形態の動作を説明する。始めに、送信側コンピュータ1において、データの作成者が、保護対象データを受信側コンピュータ2に送信する場合について説明する。

【0055】まず、作成者が保護対象データを送信しようとするときには、送信しようとする保護対象データの指定を入力するとともに、指定した保護対象データが受信側コンピュータ2に送信されたときに、保護対象データの利用許可を開始させる利用許可開始時刻と、利用許可を終了させる利用許可終了時刻とを入力する。このとき、作成者が、保護対象データの指定として保護対象デ

ータAを入力し、利用許可開始時刻として現在の時刻T₁を入力し、利用許可終了時刻として利用許可開始時刻T₁からt時間後の時刻T₁+tを入力するものとすると、利用許可開始時刻T₁および利用許可終了時刻T₁+tが設定された利用許可時間データが生成され、生成された利用許可時間データが指定した保護対象データAの先頭に付加される。

【0056】次いで、作成者は、保護対象データAを暗号化するための暗号キーを入力する。このとき、例えば、作成者の公開鍵を入力するものとすると、入力された公開鍵により、RSA暗号方式などで保護対象データAが暗号化され、受信側コンピュータ2に送信される。

【0057】一方、受信側コンピュータ2では、暗号化された保護対象データAが受信されると、受信側コンピュータ2の利用者に対して、作成者が指定した暗号キー（作成者の公開鍵）に対応した復号キーの入力が求められる。このとき、作成者から保護対象データの利用を許諾された許諾者が、許諾とともに提供された作成者の秘密鍵を入力するものとすると、入力された秘密鍵により、上記同様RSA暗号方式などで保護対象データAが復号化される。

【0058】そうすると、復号化された保護対象データAの先頭には、利用許可時間データが付加されているので、これと同一の利用許可時間データが複数生成され、これらと復号化された保護対象データAとがそれぞれ個別のファイルとして補助記憶装置8に格納される。

【0059】次に、受信側コンピュータ2において、許諾者が、このように補助記憶装置8に格納された保護対象データAを受信側コンピュータ2で利用する場合について説明する。

【0060】まず、許諾者が、例えば、保護対象データAの内容を表示したり編集したりするなど、保護対象データAを利用しようとしてアプリケーションプログラムを起動させようすると、保護対象データAの先頭には、利用許可時間データが付加されているので、この利用許可時間データおよび補助記憶装置8に格納されている複数の利用許可時間データのうち、利用許可時間幅が最短に設定されている利用許可時間データが選択され、クロックタイマ装置6から出力される時刻が取得される。

【0061】この場合に、利用許可時間データには、利用許可開始時刻T₁および利用許可終了時刻T₁+tが設定されているので、クロックタイマ装置6から出力される時刻が、利用許可時間データに設定された利用許可開始時刻T₁よりも後で、かつ、利用許可終了時刻T₁+tよりも前であるときには、利用許可時間幅にあるものとみなされ、保護対象データが消去されることなくアプリケーションプログラムが起動される。

【0062】ところが、クロックタイマ装置6から出力される時刻が、利用許可時間データに設定された利用許

11

可終了時刻 $T_1 + t$ よりも後であるとき、すなわち利用許可時間を超過しているときには、保護対象データが消去されてから、アプリケーションプログラムが起動される。

【0063】ところで、この場合に、許諾者が、作成者が設定した利用許可時間を不正に延長しようとして、クロックタイマ装置6の時刻を利用許可終了時刻 $T_1 + t$ よりも遙か前（利用許可開始時刻 T_1 よりも前）に設定したものとすると、アプリケーションプログラムを起動させるのに応じて、クロックタイマ装置6から出力される時刻が利用許可開始時刻 T_1 よりも前であると判定されるので、保護対象データが消去される。

【0064】また、許諾者が、作成者が設定した利用許可時間を不正に延長しようとして、補助記憶装置8に格納されているすべての利用許可時間データの利用許可開始時刻 T_1 または利用許可終了時刻 $T_1 + t$ を改ざんしたものとする。しかし、少なくとも保護対象データの先頭に付加されている利用許可時間データの利用許可開始時刻および利用許可終了時刻が T_1 および $T_1 + t$ のままであるので、保護対象データを消去するか否かが判定される際には、付加されている利用許可時間データが、利用許可時間幅が最短に設定されているものとして選択されることになり、初期の設定通り、クロックタイマ装置6から出力される時刻が、利用許可開始時刻 T_1 よりも前であるとき、または利用許可終了時刻 $T_1 + t$ よりも後であるときに、保護対象データが消去される。

【0065】なお、受信側コンピュータ2において、復号化された保護対象データの先頭に利用許可時間データが付加されていない場合、つまり通常のデータを復号化した場合には、利用許可時間データが生成されず、復号化された保護対象データだけがそのまま補助記憶装置8に格納される。

【0066】また、受信側コンピュータ2において、アプリケーションプログラムを起動させた場合に、保護対象データの先頭に利用許可時間データが付加されていないときには、つまり通常のデータを利用しようとする場合には、そのデータにはいかなる処理もされず、アプリケーションプログラムが起動される。

【0067】このようにして、送信側コンピュータ1において、利用許可開始時刻および利用許可終了時刻を設定した利用許可時間データを保護対象データに関連付け、これを受信側コンピュータ2に送信し、受信側コンピュータ2において、関連付けられた利用許可時間データに基づいて、クロックタイマ装置6から出力される時刻が利用許可時間幅にないときには、保護対象データを消去するようにしたから、クロックタイマ装置6の時刻が変更されても、保護対象データが時間的に無制限に利用される可能性を低減することができ、もって作成者の利益を有効に保護することができる。

【0068】特に、受信側コンピュータ2において、保

50

12

護対象データを受信するのに応じて、付加されている利用許可時間データと同一の利用許可時間データを複数生成し、保護対象データを消去するか否かの判定を、利用許可時間幅が最短に設定されている利用許可時間データに基づいて行うようにしたから、利用許可時間データが改ざんされることにより、利用許可時間を不正に延長される可能性を低減することができる。

【0069】また、送信側コンピュータ1において、保護対象データの作成者の意思に応じて、利用許可開始時刻および利用許可終了時刻を可変に設定するようにしたから、作成者が保護対象データの利用許可時間を自由に制限することができ、作成者が保護対象データを許諾者に利用させ易くなる。

【0070】さらに、送信側コンピュータ1においてではなく、受信側コンピュータ2において、ダミーとなる複数の利用許可時間データを生成するようにしたから、送信側コンピュータ1から送信するデータサイズを小さく抑えることができる。

【0071】次に、本発明の第2の実施の形態を説明する。この第2の実施の形態は、本発明に係るデータ保護装置を、受信側コンピュータ2において、クロックタイマ装置6から出力される時刻を用いずに利用許可時間が超過した保護対象データを消去するのに適用したものである。

【0072】これは、上記第1の実施の形態において、受信側コンピュータ2の演算処理装置4で、暗号化された保護対象データを入出力制御装置7で受信したときに実行させる図4(a)のフローチャートに示す処理と、保護対象データを利用するアプリケーションプログラムを起動させるのに応じて実行させる図4(b)のフローチャートに示す処理とに代えて、暗号化された保護対象データを入出力制御装置7で受信したときには、図5(a)のフローチャートに示す処理を実行し、図5(a)のフローチャートに示す処理を実行したのちには、図5(b)のフローチャートに示す割り込み処理を所定割り込み周期で実行するように構成されている。

【0073】ここで、受信側コンピュータ2の演算処理装置4において、暗号化された保護対象データを入出力制御装置7で受信したときに実行される処理は、次のように構成されている。

【0074】まず、図中、ステップS31では、復号キーをキーボード9から入力し、ステップS32に移行して、入力した復号キーで保護対象データを復号化し、ステップS33に移行して、復号化した保護対象データの先頭に利用許可時間データが付加されているか否かを判定し、付加されていると判定されたときには、ステップS34に移行するようになっている。

【0075】ステップS34では、利用許可時間データから利用許可時間を取得し、後述する図5(b)のフローチャートの割り込み処理にこれを登録し、ステップS

35に移行して、図5(b)のフローチャートの割り込み処理で計数するカウントデータを初期化し、ステップS36に移行して、復号化した保護対象データを補助記憶装置8に格納し、一連の処理を終了するようになっている。

【0076】一方、ステップS33で、復号化した保護対象データの先頭に利用許可時間データが付加されていないと判定されたときには、ステップS36に移行するようになっている。

【0077】そして、このような処理を実行したのちに所定割り込み周期で実行される割り込み処理は、次のように構成されている。まず、図中、ステップS41では、カウントデータを加算し、ステップS42に移行して、カウントデータに割り込み周期を乗じ、保護対象データが受信されてから現在に至までの経過した利用時間を算出し、ステップS43に移行するようになっている。

【0078】ステップS43では、算出した利用時間が利用許可時間を超過しているか否かを判定し、超過していると判定されたときには、ステップS44に移行して、保護対象データを消去し、一連の処理を終了するようになっている。しかし、ステップS43で、算出した利用時間が利用許可時間を超過していないと判定されたときには、一連の処理を終了するようになっている。

【0079】次に、上記第2の実施の形態の動作を説明する。まず、受信側コンピュータ2において、上記同様に送信側コンピュータ1から送信された保護対象データAが受信されると、受信側コンピュータ2の利用者に対して、復号キーの入力が求められる。このとき、許諾者が、作成者の秘密鍵を入力するものとすると、入力された秘密鍵により保護対象データAが復号化される。

【0080】そうすると、復号化された保護対象データAの先頭には、利用許可時間データが付加されているので、利用許可時間データから利用許可時間が取得され、これが図5(b)の割り込み処理に登録されるとともに、図5(b)の割り込み処理で計数されるカウントデータに初期値として“0”が設定される。そして、復号化した保護対象データAが補助記憶装置8に格納される。

【0081】その後に、所定割り込み周期T₁で図5(b)の割り込み処理が実行され、割り込み周期ごとに、カウントデータが加算され、カウントデータに割り込み周期T₁を乗じることにより利用時間が算出される。そして、この利用時間が、登録された利用許可時間を超過していると判定されたときには、保護対象データAが消去される。

【0082】ところで、この場合に、許諾者が、作成者が設定した利用許可時間を不正に延長しようとして、付加されている利用許可時間データを改ざんしたものとする。しかし、受信すると同時に、利用許可時間データに

設定されている利用許可時間が図5(b)の割り込み処理に登録され、この割り込み処理では、登録された利用許可時間に基づいて、保護対象データが消去されるようになっているので、初期に設定した利用許可時間通り、保護対象データが消去される。

【0083】このようにして、所定割り込み周期による割り込み処理で、利用許可時間が超過したか否かを常に監視するようにしたから、クロックタイマ装置6から出力される時刻によらず、利用許可時間を超過した保護対象データを即時に消去することができ、保護対象データが時間的に無制限に利用される可能性をより低減することができ、もって作成者の利益を有効に保護することができる。

【0084】特に、保護対象データを受信すると同時に、付加されている利用許可時間データから利用許可時間を取得し、取得した利用許可時間を割り込み処理に登録し、割り込み処理では、登録された利用許可時間に基づいて、保護対象データを消去するようにしたから、利用許可時間が延長される可能性を低減することができる。

【0085】なお、上記実施の形態においては、利用許可時間データを保護対象データの先頭に付加するように構成したが、これに限らず、利用許可時間データを保護対象データの内部や末尾に付加するように構成したり、また、保護対象データとは別のデータとして利用許可時間データを生成し、保護対象データに利用許可時間データのリンク先を保持させておくように構成したりしてもよい。

【0086】また、上記実施の形態においては、利用許可時間データに利用許可開始時刻および利用許可終了時刻を直接設定するように構成したが、これに限らず、受信側コンピュータ2では、例えば、Aなら1時間、Bなら3時間、Cなら10時間といった具合に、あらかじめ利用許可時間をいくつかの段階に区分して管理するようにし、送信側コンピュータ1では、受信側コンピュータ2で段階的に管理されている利用許可時間を特定するようなデータ（この場合には、A～Cのいずれかのデータ）を利用許可時間データに設定するように構成してもよい。このような構成であれば、利用許可時間データに利用許可時間を直接設定しないので、利用許可時間データの内容が解読され、改ざんされる可能性を低減することができる。

【0087】さらに、上記実施の形態においては、利用許可を開始させる利用許可開始時刻および利用許可を終了させる利用許可終了時刻を利用許可時間データに設定し、利用許可開始時刻および利用許可終了時刻に基づいて、保護対象データを消去するか否かを判定するように構成したが、これに限らず、送信側コンピュータ1では、利用許可時間幅（例えば、t時間）を利用許可時間データに設定して送信し、受信側コンピュータ2で保護

15

対象データを受信したときに、受信した時の時刻を利用許可開始時刻として利用許可時間データに設定し、この利用許可開始時刻と利用許可時間幅とから利用許可終了時刻を算出し、算出した利用許可終了時刻および利用許可開始時刻に基づいて、保護対象データを消去するか否かを判定するように構成してもよい。

【0088】さらに、上記実施の形態においては、受信側コンピュータ2において、ダミーとなる複数の利用許可時間データを生成する処理を実行するように構成したが、これに限らず、送信側コンピュータ1において、利用許可時間データを保護対象データに付加するときに、ダミーとなる複数の利用許可時間データを生成する請求項2記載の利用許可時間データ関連付手段としての処理を実行し、これらをまとめて受信側コンピュータ2に送信するように構成してもよい。

【0089】さらに、上記実施の形態においては、ダミーとなる複数の利用許可時間データを生成するように構成したが、これに限らず、特に、ダミーとなる複数の利用許可時間データを生成しないように構成してもよい。

【0090】さらに、上記実施の形態においては、利用許可時間データが不正に改ざんされた場合について、特に処理をしないように構成したが、これに限らず、利用許可時間データが不正に改ざんされたと判定されたときには、例えば、すべての利用許可時間データを利用許可時間幅が最短に設定されている利用許可時間データに書き換えたり、保護対象データを消去したりする処理を実行するように構成してもよい。このような構成であれば、利用許可時間データが不正に改ざんされる可能性をより低減することができる。

【0091】さらに、上記実施の形態においては、送信側コンピュータ1で保護対象データを暗号化して送信するように構成したが、これに限らず、保護対象データを特に暗号化せずに送信するように構成してもよい。

【0092】さらに、上記実施の形態においては、送信側コンピュータ1で、利用許可時間データを保護対象データに付加して送信し、受信側コンピュータ2で、保護対象データを利用しようとするときに、付加されている利用許可時間データに基づいて、保護対象データを消去するように構成したが、これに限らず、一台のコンピュータ内で、これら一連の処理を実行するように構成してもよい。

【0093】さらに、上記実施の形態においては、特に利用許可時間データに設定されている利用許可開始時刻を再設定しないように構成したが、これに限らず、アプリケーションプログラムを起動させるのに応じて、利用許可開始時刻を、クロックタイマ装置6から取得した現在の時刻に再設定するように構成してもよい。このような構成であれば、あらかじめ設定された利用許可時間からすでに利用した利用経過時間を減算したものを新たな利用許可時間として再設定することになり、この新たな

10

20

30

40

50

16

利用許可時間に基づいて、保護対象データを消去するようすれば、クロックタイマ装置の時刻が変更されることにより、利用許可時間が不正に延長される可能性を低減することができる。

【0094】さらに、上記実施の形態において、図3、図4および図5のフローチャートに示す処理を実行するにあたってはいずれも、主記憶装置5のROMにあらかじめ格納されているプログラムを実行する場合について説明したが、これに限らず、これらの手順を示したプログラムが記録された記録媒体から、そのプログラムを主記憶装置5のRAMに読み込んで実行するようにしてもよい。

【0095】ここで、記録媒体とは、RAM、ROM、FD、コンパクトディスク、ハードディスク、光磁気ディスクまたは紙等の記録媒体であって、電子的、磁気的、光学的等の読み取り方法のいかんにかかわらず、コンピュータで読み取り可能な記録媒体であれば、あらゆる記録媒体を含むものである。

【0096】さらに、上記実施の形態において、図3、図4および図5のフローチャートに示す処理はいずれも、ソフトウェアで構成した場合について説明したが、これに代えて、比較回路、演算回路、論理回路等の電子回路を組み合わせるよう構成してもよい。

【0097】上記実施の形態において、ステップS4およびS5は、請求項1、3または4記載の利用許可時間データ関連付手段に対応し、ステップS2からS5までは、請求項5記載の利用許可時間データ関連付手段に対応し、ステップS25からS28までは、請求項1または3記載の保護対象データ消去手段に対応し、ステップS24からS28までは、請求項2または4記載の保護対象データ消去手段に対応し、ステップS14およびS15は、請求項4記載の第2の利用許可時間データ関連付手段に対応している。

【0098】

【発明の効果】以上説明したように、本発明に係るデータ保護装置によれば、クロックタイマ装置の時刻が変更されても、保護対象データが時間的に無制限に利用される可能性を低減することができ、もって作成者の利益を有効に保護することができるという効果が得られる。

【0099】また、本発明に係る請求項2または4記載のデータ保護装置によれば、利用許可時間データが改ざんされることにより、利用許可時間が不正に延長される可能性を低減することができるという効果も得られる。

【0100】さらに、本発明に係る請求項5記載のデータ保護装置によれば、作成者または所有者が保護対象データの利用許可時間を自由に制限することができるから、作成者または所有者が保護対象データを許諾者に利用させ易くなるという効果も得られる。

【0101】さらに、本発明に係る請求項6記載のデータ保護装置によれば、クロックタイマ装置の時刻が変更

17

されることにより、利用許可時間が不正に延長される可能性を低減することができるという効果も得られる。

【図面の簡単な説明】

【図1】実施の形態の構成を示すブロック図である。

【図2】図1における送信側コンピュータおよび受信側コンピュータの構成を示すブロック図である。

【図3】送信側コンピュータで実行される処理を示すフローチャートである。

【図4】受信側コンピュータで実行される第1の処理を示すフローチャートである。

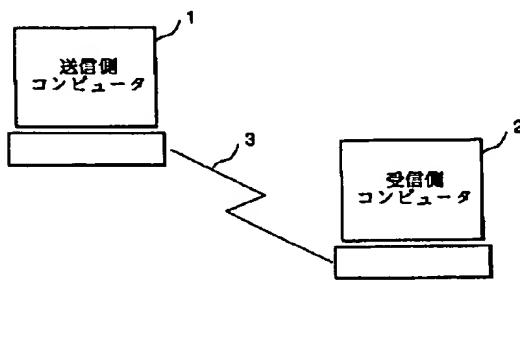
【図5】受信側コンピュータで実行される第2の処理を*

*示すフローチャートである。

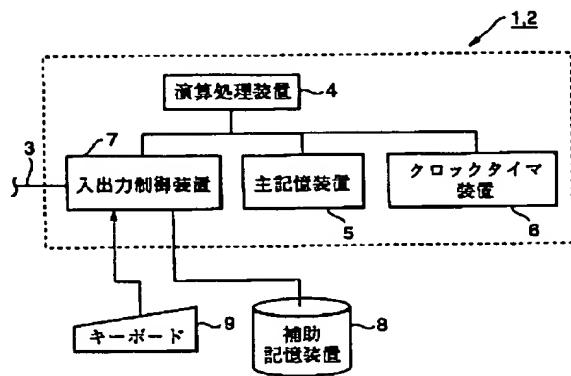
【符号の説明】

1	送信側コンピュータ
2	受信側コンピュータ
3	データ伝送路
4	演算処理装置
5	主記憶装置
6	クロックタイマ装置
7	入出力制御装置
8	補助記憶装置
9	キーボード

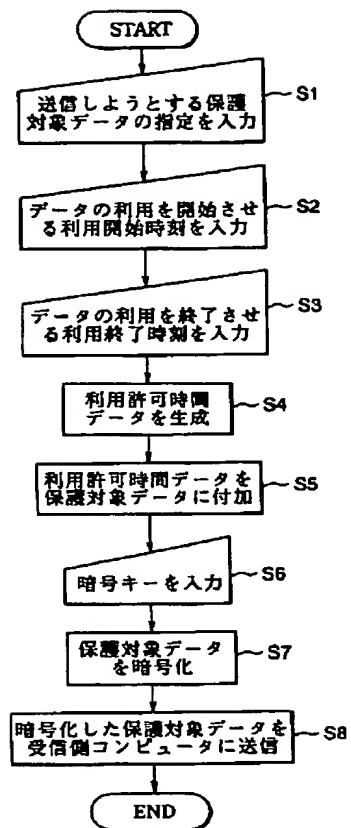
【図1】



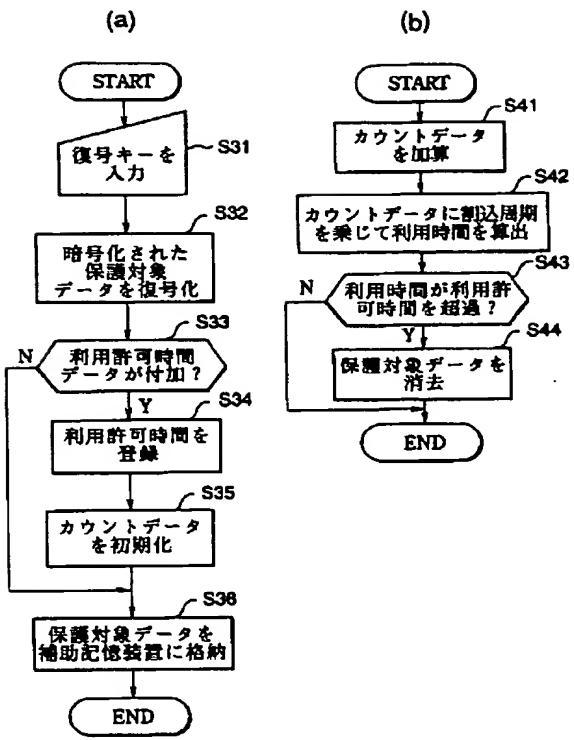
【図2】



【図3】



【図5】



【図4】

